UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/751,576	12/29/2000	Lok Yan Leung	AUS920000797US1	8367

35525 7590 01/30/2012

IBM CORP (YA)
C/O YEE & ASSOCIATES PC
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER	
LIPMAN, JACOB	
ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
01/30/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptonotifs@yeeiplaw.com
mgamez@yeeiplaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte LOK YAN LEUNG, ANTHONY JOESPH NADALIN, BRUCE ARLAND RICH, and THEODORE JACK LONDON SHRADER

Appeal 2009-013393
Application 09/751,576
Technology Center 2400

Before DENISE M. POTHIER, JEFFREY S. SMITH, and ERIC B. CHEN, *Administrative Patent Judges*.

SMITH, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

This is an appeal under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1, 2, 4-21, and 23-32, which are all the claims remaining in the application. Claims 3 and 22 have been cancelled. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

Invention

Appellants' invention relates to a method for managing access to data in a keystore in a data processing system. A request for access to an item of data is received from a requestor, wherein the item of data is encrypted using a key. A determination of whether the requestor is a trusted requestor is made. The key and the item of data are sent to the requestor in response to a determination that the requestor is a trusted requestor. Abstract.

Representative Claim

1. A method in a data processing system for managing access to data in a keystore, the method comprising:

receiving a request for access to an item of data from a requestor, wherein the item of data is encrypted using a first key;

determining whether the requestor is a trusted requestor, wherein the determining step is performed by checking a requestor's identity against a trusted codebase;

responsive to a determination that the requestor is a trusted requestor, decrypting a copy of the item of data using a second key to form a decrypted item of data; and

sending the decrypted item of data to the requestor.

Prior Art

Cane	US 5,940,507	Aug. 17, 1999
Padgett	US 6,167,518	Dec. 26, 2000

Examiner's Rejections

Claims 1, 2, 4-21, and 23-32 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Cane and Padgett.

Claim Groupings

We decide the appeal on the basis of claims 1, 4, 6, 7, and 11.

PRINCIPAL ISSUE

Did the Examiner err in finding that the combination of Cane and Padgett teaches "determining whether the requestor is a trusted requestor, wherein the determining step is performed by checking a requestor's identity against a trusted codebase" and "responsive to a determination that the requestor is a trusted requestor, decrypting a copy of the item of data using a second key to form a decrypted item of data" as recited in claim 1?

ANALYSIS

Section 103 rejection of claims 1, 2, 5, 8-10, 12, 14, 20, 21, 27-29, and 32

Appellants contend that Cane does not teach "responsive to a determination that the requestor is a trusted requestor, decrypting a copy of the item of data using a second key to form a decrypted item of data" as

recited in claim 1. App. Br. 17-22; Reply Br. 4-5. According to Appellants, Cane teaches encrypting a file with a secondary key, then encrypting the secondary key with a master key. The encrypted file and encrypted secondary key are sent to an archive server. To recover an encrypted file, the encrypted file and the encrypted key are sent from the archive server to the client. The master key is used to decrypt the secondary key, then the secondary key is used to decrypt the file. App. Br.19.

We find that the encrypted file that is retrieved from the archive file by the client is "a copy" of the encrypted file within the meaning of claim 1. Decrypting the copy of the encrypted file using the master key to decrypt the secondary key then using the secondary key to decrypt the file as taught by Cane teaches "decrypting a copy of the item of data using a second key to form a decrypted item of data" within the meaning of claim 1.

Appellants contend that Cane does not teach a "trusted requestor," therefore, Cane cannot teach "responsive to a determination that the requestor is a trusted requestor" as recited in claim 1. App. Br. 22-23. Appellants also contend that neither Cane nor Padgett teach "determining whether the requestor is a trusted requestor, wherein the determining step is performed by checking a requestor's identity against a trusted codebase." App. Br. 24-25.

Appellants' contentions are inconsistent with Appellants' admissions on page 10, lines 2-19of the Specification that determining whether a requestor is trusted can be made by various security checks well known in the art. Also, the Examiner finds that Padgett teaches determining whether a requestor is a trusted requestor by checking a requestor's identity against a trusted database. Ans. 4, 5-6. The Examiner further finds that Cane teaches

authentication measures, and that one of skill in the art would have recognized that authentication measures include comparing a user's name and password against an authorized list. Ans. 5-6. We agree with the findings and conclusion made by the Examiner.

We sustain the rejection of claim 1 under 35 U.S.C. § 103. Appellants do not present arguments for separate patentability of claims 2, 5, 8-10, 12, 14, 20, 21, 24, 27-29, and 32, which fall with claim 1.

Section 103 rejection of claims 4 and 23

Appellants contend that Cane does not teach "wherein the item of data is another key" as recited in claim 4. App. Br. 26. We observe that "the item of data is another key" as recited in claim 4 is a description of the item that does not alter any steps or structural elements of the method recited in claim 4. The "item of data is another key" is therefore non-functional descriptive material that does not distinguish the claim from the prior art in terms of patentability. *See In re Ngai*, 367 F.3d 1336, 1339 (Fed. Cir. 2004). *Cf. In re Gulack*, 703 F.2d 1381, 1385 (Fed. Cir. 1983). *See also Ex Parte Nehls*, 88 USPQ2d 1883, 1887-90 (BPAI 2008)(precedential). We sustain the rejection of claims 4 and 23 under 35 U.S.C. § 103.

Section 103 rejection of claims 6 and 25

Appellants contend that Cane does not teach "the item of data is indexed within the Keystore using an alias" as recited in claim 6. According to Appellants, Cane teaches storing the location of the encrypted file in the archive server in an index, but does not teach indexing using an alias. App. Br. 26-27. The scope of "alias" recited in claim 6 encompasses information.

Appellants have not provided evidence or persuasive argument to distinguish an "item of data" that "is indexed … using an alias" from an encrypted file that is indexed using the key's name and location as taught by Cane (col. 4, ll. 37-41). We sustain the rejection of claims 6 and 25 under 35 U.S.C. § 103.

Section 103 rejection of claims 7, 13, and 26

Appellants contend that Cane does not teach "responsive to an absence of a determination that the requestor is a trusted requestor, returning a null result to the requestor" as recited in claim 7, because Cane does not teach a trusted requestor as recited in claim 1. App. Br. 27. We find this argument unpersuasive for the reasons given in the analysis of claim 1. We sustain the rejection of claims 7 and 26 under 35 U.S.C. § 103. Appellants present arguments for claim 13 (App. Br. 27-28) similar to those presented for claim 6 which we find unpersuasive.

Section 103 rejection of claims 11, 15-19, 30, and 31

Appellants contend that Cane does not teach "determining whether the requestor is a trusted requestor, wherein the determining step is performed by checking a requestor's identity against a trusted codebase" as recited in claim 11. App. Br. 29. We find this argument unpersuasive for the reasons given in the analysis of claim 1.

Appellants contend that Cane does not teach "responsive to a determination that the requestor is a trusted requestor, sending a second key and an encrypted copy of the item of data to the requestor" as recited in claim 11. App. Br. 29. We find that retrieving the encrypted file and

retrieving the master key from the memories of Cane teaches "sending a second key and an encrypted copy of the item of data to the requestor" within the meaning of claim 11. We sustain the rejection of claims 11, 15-19, 30, and 31 under 35 U.S.C. § 103, which are not argued separately (App. Br. 30).

CONCLUSION

The Examiner did not err in finding that the combination of Cane and Padgett teaches "determining whether the requestor is a trusted requestor, wherein the determining step is performed by checking a requestor's identity against a trusted codebase" and "responsive to a determination that the requestor is a trusted requestor, decrypting a copy of the item of data using a second key to form a decrypted item of data" as recited in claim 1.

DECISION

The rejection of claims 1, 2, 4-21, and 23-32 under 35 U.S.C. § 103(a) as being unpatentable over Cane and Padgett is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 41.50(f).

AFFIRMED

tj